

IN THE SPECIFICATION

Please amend the paragraph at page 3, beginning at line 17 as follows:

In this aspect, the source of a data packet may be authenticated with a reasonable degree of security without the data processing overhead inherent in digital signature techniques. The authentication technique of the present invention is not required to protect the content of a data packet against alteration, only to provide an indication that the packet was sent by a valid first server. The data processing involved at a first server in selecting a data element from a stored list and including the data element in a data packet before sending it is potentially very small. Method steps (iii) and (iv) may be repeated in respect of each subsequently received packet to be forwarded, until all data elements in the list sent at step (ii) have been used or until a predetermined minimum number of data elements remain unused. At this point, a further list of data elements may be stored or otherwise obtained and a copy of the further list sent to authorized recipients according to method steps (i) and (ii), before forwarding further packets.

Please amend the paragraphs at page 7, beginning at line 17 through line 20 as follows:

Figures 1A and 1B are ~~1 is a~~ flow diagrams showing ~~an~~ initial sequences of steps in a method according to embodiments of the present invention for sending and receiving respectively; and

Figures 2A and 2B are ~~2 is a~~ flow diagrams showing a further sequences of steps in a method according to embodiments of the present invention for sending and receiving respectively.

Please amend paragraph at page 7, at lines 21 through 30, as follows:

Referring to Figures 1A and 1B, two flow diagrams are presented, Figure 1A showing the initial steps in operation of a first server to enable packets to be routed under the control of a packet authentication method according to embodiments of the present invention, Figure 1B showing the initial steps in operation of a recipient server, co-operating with the first server, to enable packets routed by the first server to be received and verified as originating from the first server. In the particular embodiment to be described, an encryption technique based upon public and private encryption keys is used during the initial processing steps shown in Figures 1A and 1B, using PGP for example as referenced above, although any secure method for transmitting data may be used.